

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

LEO GUY, et al.,

Plaintiffs,

v.

CONVERGENT OUTSOURCING,
INC.,

Defendant.

CASE NO. C22-1558 MJP

ORDER GRANTING IN PART AND
DENYING IN PART
DEFENDANT'S MOTION TO
DISMISS

This matter comes before the Court on Defendant Convergent Outsourcing, Inc.'s Motion to Dismiss. (Dkt. No. 36.) Having reviewed the Motion, the Response (Dkt. No. 43), the Reply (Dkt. No. 44), and all supporting materials, the Court GRANTS in part and DENIES in part the Motion to Dismiss.

BACKGROUND

Convergent Outsourcing, Inc. is a third-party consumer debt collector that provides its services to the telecommunication, utility, banking, cable, and financial services industries.

(Consolidated Amended Complaint ¶ 1 (Dkt. No. 31).) Convergent’s computer system “holds and stores certain highly sensitive personally identifiable information (‘PII’ or ‘Private Information’) of Plaintiffs and the putative Class Members, who are customers of companies for which Convergent provides debt collection services, i.e., individuals who provided their highly sensitive and private information in exchange for business services.” (Id. ¶ 3.) PII includes consumer first and last names, home and email addresses, phone numbers, Social Security numbers, employers, financial account numbers, and bank account or payment card information. (Id. ¶ 44.) Of note, Plaintiffs do not allege a business relationship with Convergent and they are not alleged to be customers of Convergent. (See id. ¶¶ 26, 36-37.) Rather, Plaintiffs allege that “Convergent collects Private Information of consumers from companies seeking Convergent’s debt collection services.” (Id. ¶ 36.) And it is through those businesses that Convergent came into possession of Plaintiffs’ PII.

On June 17, 2022, Convergent learned that its computer system was breached by a third-party, who accessed and exfiltrated the PII of 640,906 individuals, including Plaintiffs. (CAC ¶¶ 46, 49.) But Convergent did not notify the affected individuals until late October 2022. (Id. ¶¶ 48-49.) Plaintiffs allege that the PII stolen was unencrypted and improperly safeguarded. (Id. ¶¶ 53-54.) Plaintiffs allege that Convergent failed to protect their PII and follow minimum industry standards. (See id. ¶¶ 45, 54, 58-63, 78, 81-85.)

To satisfy concerns about standing and injury, Plaintiffs provide allegations about the value of their PII and the other injuries they have suffered. First, Plaintiffs allege that as a result of the Convergent data breach their PII has lost economic value because it is now readily available, and they received nothing in return for its disclosure. (CAC ¶ 90.) Plaintiffs allege on information and belief that their PII is now available for sale on the “Dark Web,” (id. ¶ 55), and

that it may have a value ranging from \$40 to \$363, depending on the sensitivity of the information, (id. ¶¶ 86, 88). Plaintiffs also allege that there is an “active and robust legitimate market,” which is referred to as the “data brokering industry,” through which individuals can sell their person data for up to \$50 a year. (id. ¶ 89.) Plaintiff Guy believes his PII has already been sold to criminals, given that he now receives many spam phone calls and emails daily after the data breach, but not before. (Id. ¶¶ 125-29.) Second, Plaintiffs allege that they have spent time trying to monitor fraudulent activity arising from the data breach. (See id. ¶¶ 125, 127-28.) This includes Plaintiff Tanner who found \$100 fraudulent charge on Netflix that he spent several hours disputing (though he does not allege any out-of-pocket costs). (Id. ¶ 153.) Plaintiffs admit that Convergent has offered some identity theft monitoring services, but assert that it is only a “limited subscription” that will expire and will require them to pay for additional credit monitoring out of pocket. (Id. ¶ 98.)

Plaintiffs seek to represent a class of similarly-situated individuals and they bring the following claims: (1) negligence; (2) breach of implied contract; (3) breach of confidence; (4) invasion of privacy; (5) unjust enrichment; (6) violations of Washington’s Consumer Protection Act violations; (7) violations of Washington’s data breach laws, RCW 19.255.010(2); (8) violations of California’s Consumer Privacy Act; (9) violations of California’s Unfair Competition Law; (10) invasion of privacy under California’s Constitution Art. 1, § 1; and (11) declaratory judgment. (CAC ¶¶ 193-329.) Convergent seeks dismissal of all claims.

ANALYSIS

A. Legal Standard

Convergent moves to dismiss under Rule 12(b)(6), not Rule 12(b)(1). Accordingly, the Court considers Convergent’s argument concerning Plaintiffs’ standing as a challenge to the

sufficiency of the pleadings as to each claim. Under Fed. R. Civ. P. 12(b)(6), the Court may dismiss a complaint for “failure to state a claim upon which relief can be granted.” In ruling on a motion to dismiss, the Court must construe the complaint in the light most favorable to the non-moving party and accept all well-pleaded allegations of material fact as true. Livid Holdings Ltd. v. Salomon Smith Barney, Inc., 416 F.3d 940, 946 (9th Cir. 2005); Wylar Summit P’ship v. Turner Broad. Sys., 135 F.3d 658, 661 (9th Cir. 1998). Dismissal is appropriate only where a complaint fails to allege “enough facts to state a claim to relief that is plausible on its face.” Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007). A claim is plausible on its face “when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009).

B. Negligence

Convergent challenges Plaintiffs’ negligence claim, arguing that Plaintiffs have failed to identify a duty, damages, or causation. The Court agrees that Plaintiffs have not identified an actionable duty and DISMISSES the claim. The Court does not reach the question of damages or causation.

“In order to prove actionable negligence, a plaintiff must establish the existence of a duty, a breach thereof, a resulting injury, and proximate causation between the breach and the resulting injury.” Schooley v. Pinch’s Deli Mkt., Inc., 134 Wn.2d 468, 474 (1998). “In a negligence action the threshold question is whether the defendant owes a duty of care to the injured plaintiff,” and “[t]he existence of a legal duty is a question of law.” Id. The existence of a duty “is a question of law and depends on mixed considerations of logic, common sense, justice, policy, and precedent.” Snyder v. Med. Serv. Corp., 145 Wn.2d 233, 243 (2001).

1 Plaintiffs identify what they believe to be three independent sources of a duty: (1) tort
 2 law; (2) statutory law; and (3) property law. The Court analyze these three alleged duties and
 3 find them inadequate to form a legal duty.

4 **1. Common law tort duty to prevent third-party acts**

5 “As a general rule, in the absence of a special relationship between the parties, there is no
 6 duty to control the conduct of a third person so as to prevent him from causing harm to another.”
 7 Robb v. City of Seattle, 176 Wn.2d 427, 433 (2013) (citation and quotation omitted). “Actors
 8 have a duty to exercise reasonable care to avoid the foreseeable consequences of their acts.”
 9 Washburn v. City of Fed. Way, 178 Wn.2d 732, 757 (2013) (citing Restatement (Second) of
 10 Torts § 281 cmts. c, d (1965)). “This duty requires actors to avoid exposing another to harm from
 11 the foreseeable conduct of a third party.” Id. (citing Restatement § 302). And while criminal acts
 12 of third parties are generally unforeseeable, there can be a duty to protect against such acts in
 13 limited circumstances. Id.

14 Plaintiffs focus on the Washington Supreme Court’s recognition under Restatement
 15 (Second) of Torts § 302B that “a duty to third parties may arise in the limited circumstances that
 16 the actor’s own affirmative act creates a recognizable high degree of risk of harm.” Robb, 176
 17 Wn.2d at 433. (citation and quotation omitted). “Specifically, Restatement § 302B provides that
 18 ‘[a]n act or an omission may be negligent if the actor realizes or should realize that it involves an
 19 unreasonable risk of harm to another through the conduct of the other or a third person which is
 20 intended to cause harm, even though such conduct is criminal.’” Id. at 434 (quoting Restatement
 21 § 302B). But “[t]he fact that the actor realizes or should realize that action on his part is
 22 necessary for another’s aid or protection does not of itself impose upon him a duty to take such
 23 action.” Restatement § 314. “[U]nder [Restatement] § 314, an actor might still have a duty to
 24

1 take action for the aid or protection of the plaintiff in cases involving misfeasance (or affirmative
 2 acts), where the actor's prior conduct, whether tortious or innocent, may have created a situation
 3 of peril to the other." Robb 176 Wn.2d at 436. "Liability for nonfeasance (or omissions), on the
 4 other hand, is largely confined to situations where a special relationship exists." Id.

5 The only Washington appellate decision the Parties identify that has imposed a duty
 6 owed for the criminal acts of a third party is Parrilla v. King County, 138 Wn. App. 427 (2007).
 7 In Parilla, a County bus driver exited the bus with the engine running, which allowed a visibly
 8 erratic passenger to commandeer the vehicle. The Court concluded that the County owed a duty
 9 to third parties harmed by the passenger-driven bus because "the affirmative acts of the bus
 10 driver and the foreseeability and magnitude of the risk created by the driver," "justified imposing
 11 a duty under § 302B comment e." Robb, 176 Wn.2d at 435.

12 Plaintiffs fail to convince the Court that Convergent engaged in misfeasance sufficient to
 13 impose a duty to protect against the theft of their PII from Convergent's computer system. (Resp.
 14 at 5.) Plaintiffs argue that "Convergent committed affirmative misfeasance by utilizing faulty,
 15 unsecure computer systems and by collecting and storing Plaintiffs' Private Information on its
 16 systems in an unencrypted format, all of which was inconsistent with industry standards, paving
 17 the way for a criminal data breach to result in harm to Plaintiffs and Class members." (Id.) These
 18 allegations are inadequate to show affirmative misfeasance. See Veridian Credit Union v. Eddie
 19 Bauer, LLC, 295 F. Supp. 3d 1140, 1157 (W.D. Wash. 2017). In Veridian, the plaintiffs alleged
 20 that:

21 Eddie Bauer failed to "maintain adequate data security measures, implement best
 22 practices, upgrade security systems, and comply with industry standards," "implement
 23 chip-based card technology, otherwise known as EMV technology," "take reasonable
 24 steps to protect its computer systems from being breached," "timely upgrade its POS
 software to remedy security vulnerabilities," "take reasonable steps to upgrade and
 protect Payment Card Data," "ensure that its IT systems were adequately secured,"

“make necessary changes to its security practices and protocols,” “take necessary measures to maintain an adequate firewall,” [and] “comply with industry standards for data security[.]”

Id. at 1158. Plaintiffs’ claims are indistinguishable from the same acts found in Veridian to be inadequate to show an affirmative misfeasance. The allegations point to omissions, not active misfeasance. And Plaintiffs’ allegations fail to approach those in Parilla, where the driver abandoned his running bus and allowed a visibly erratic passenger to commandeer it. Parrilla, 138 Wn. App. at 439. There are no comparable allegations here that might suggest Convergent undertook some affirmative act in the face of an obvious threat. The Court finds Plaintiffs’ allegations of a duty inadequate.

2. Statutory duty

Plaintiffs unpersuasively invoke Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as the basis of a duty Convergent owed to maintain reasonable cybersecurity measures.

Although Washington does not permit negligence per se claims, it does allow a duty to be formulated from a statute. Jackson v. City of Seattle, 158 Wn. App. 647, 651, 244 P.3d 425, 428 (2010)). To determine whether a statute imposes a legal duty, Washington follows Restatement (Second) of Torts § 286 (1965). See Hansen v. Friend, 118 Wn.2d 476, 480–81 (1992). Under the Restatement’s test, “[t]he court may adopt as the standard of conduct of a reasonable [person] the requirements of a legislative enactment” but only if the law’s “purpose is found to be exclusively or in part”:

- (a) to protect a class of persons which includes the one whose interest is invaded, and
- (b) to protect the particular interest which is invaded, and
- (c) to protect that interest against the kind of harm which has resulted, and
- (d) to protect that interest against the particular hazard from which the harm results.

Id. at 480–81 (quoting Restatement (Second) of Torts § 286 (1965)).

1 As a statutory source of a duty, Plaintiffs invoke Section 5 of the FTC Act, which
 2 generally forbids unfair and deceptive acts or practices affecting commerce. See 15 U.S.C. § 45.
 3 And Plaintiffs note that the Third Circuit has concluded that the failure to provide adequate
 4 cybersecurity and to prevent consumer data hacking can form the basis of a Section 5 claim.
 5 F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015).

6 Plaintiffs do not provide a persuasive argument as to why Section 5 of the FTC Act
 7 imposes a duty on Convergent. First, Plaintiffs offer no analysis of how or why Section 5 of the
 8 FTC Act satisfies all four Restatement § 268 requirements. Plaintiffs do identify the Third
 9 Circuit’s decision in Wyndham. But that decision provides no salient analysis of the purpose of
 10 the FTC Act and why it would apply to the facts alleged here. Second, Plaintiffs offer no
 11 Washington cases imposing a duty under Section 5 of the FTC Act. Instead, Plaintiffs rely on
 12 three district court decisions, none of which fills the void because they either do not analyze the
 13 issue under Restatement § 268 or they fail to provide any analysis of the FTC Act. See In re Cap.
 14 One Consumer Data Sec. Breach Litig., 488 F. Supp. 3d 374, 408 (E.D. Va. 2020) (providing no
 15 analysis of the FTC Act or Restatement § 268); In re Equifax, Inc., Customer Data Security
 16 Breach Litig., 362 F. Supp. 3d 1295, 1327 (N.D. Ga. 2019) (considering a negligence per se
 17 claim under Georgia law and glibly concluding that “Plaintiffs are within the class of persons
 18 intended to be protected by the statute, and that the harm suffered is the kind the statute meant to
 19 protect.”); In re Marriott Int’l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 479
 20 (D. Md. 2020) (same).

21 Defendants have the better argument, and rely on Veridian, which rejected Plaintiffs’
 22 same claim under Washington law. See Veridian, 295 F. Supp. 3d at 1159. In Veridian, the Court
 23 explained that the FTC Act protects “the public from the evils likely to result from the
 24

destruction of competition or the restriction of it in a substantial degree,” id. (quoting FTC v. Raladam Co., 283 U.S. 643, 647–48 (1931)), and that “‘Section 5 in particular seeks to protect consumer[s] and competitor[s] from unfair trade practice[s],” id. (quoting SELCO Cmty. Credit Union v. Noodles & Co., 267 F. Supp. 3d 1288, 1296 (D. Colo. 2017)). The Court concluded that those harmed by the defendant’s failure to secure PII did not fall within the FTC Act’s purpose of protecting against unfair competition. Id. Although the Court in Veridian did not analyze whether the Act’s focus on deceptive acts could provide a fit, the Court here finds see no reason why it would, given the facts alleged by Plaintiffs. The Court agrees with the analysis in Veridian and holds that Plaintiffs have failed to show how Section 5 of the FTC Act is intended to protect Plaintiffs from the loss of PII due to a cybersecurity breach caused by a third party.

The Court finds that the FTC Act cannot form the basis of the alleged duty.

3. Property-related duty

Lastly, Plaintiffs invoke a limited duty owed by landowners to third parties to argue that Convergent owed them a similar duty. This is unconvincing.

The Washington Supreme Court has recognized a duty “[w]here property of which the actor has possession or control affords a peculiar temptation or opportunity for intentional interference likely to cause harm.” Hutchins v. 1001 Fourth Ave. Assocs., 116 Wn.2d 217, 230–31 (1991) (quoting Restatement (Second) of Torts § 302B)). The Court explained that “[a] duty may also exist where defendant affirmatively brings about ‘an especial temptation and opportunity for criminal misconduct’ which will give rise to a duty on defendant’s part to take precautions against it.” Id. at 230 (quotation omitted). As an illustration, the Court imagined that a landowner may owe a duty of care to children who find dynamite caps in an open box next to a playground. Id.

Plaintiffs offer no reason why this case has application to the allegations in the Consolidated Amended Complaint, and the Court finds none. In substance, Hutchins merely applies the same logic the court followed in Parilla. That is, if one creates an unreasonably dangerous situation or an “especial temptation,” it may form the basis of negligence. But Plaintiffs fail to identify any facts that would support finding Convergent created a particular, “especial temptation.” At best, they argue that “Private Information . . . presents a temptation for theft” and “Convergent’s computer system” afforded the temptation to access it. (Resp. at 8.) But these allegations do not identify a unique or heightened temptation, such as dynamite caps in a park or an object of special allure to theft. Businesses routinely store PII, and Plaintiffs fail to explain why Convergent created an “especial temptation” by its failure to safeguard the PII. The Court declines to impose a duty on this theory

* * *

The Court GRANTS the Motion as to the negligence claim and DISMISSES it for lack of an actionable duty.

C. Breach of Implied Contract

Plaintiffs allege that Convergent breached an implied contract whereby they gave Convergent “or its third-party agents in exchange for Convergent’s services or employment” and Convergent promised to protect their PII from unauthorized disclosure. (CAC ¶ 223.) The Court agrees with Convergent that this claim is flawed.

“A contract implied in fact . . . is an agreement depending for its existence on some act or conduct of the party sought to be charged and arising by implication from circumstances which, according to common understanding, show a mutual intention on the part of the parties to contract with each other.” Young v. Young, 164 Wn.2d 477, 485 (2008) (citation and quotation

omitted). Where a contract is implied in fact, there lies a claim of quantum meruit, which “is the method of recovering the reasonable value of services provided under a contract implied in fact.”

Id.

Convergent convincingly argues that there are no allegations in the Consolidated Amended Complaint that might suggest a mutual intention to contract, given the lack of a bilateral relationship concerning Plaintiffs’ PII. (Mot. at 11 (citing CAC ¶¶ 227, 229).) Convergent is not alleged to have any direct relationship to Plaintiffs, which is fatal to this claim. Convergent is instead alleged to be a “third-party debt collection company that serves the telecommunication, utility, banking, cable company, and financial service industries.” (CAC ¶ 1.) Plaintiffs “are customers of companies for which Convergent provides debt collection services, i.e., individuals who provided their highly sensitive and private information in exchange for business services.” (Id. ¶ 3.) And although Plaintiffs allege that they were “required to provide their Private Information to Defendant as a condition of receiving other services provided by Defendant,” they do not identify any business relationship between them and Convergent. (Id. ¶ 222.) Most important, there are no specific facts about exactly how or why Plaintiffs gave Convergent their PII, how Convergent got the PII, or what interactions any Plaintiff had with Convergent. These allegations are inadequate to show a mutual intention to contract.

Plaintiffs are correct that some courts have found the receipt of PII sufficient to show an implied-in-fact contract. But each of the cases Plaintiffs cite involve a direct transfer of PII through an existing, direct consumer or employee relationship. (See Opp. at 11 (citing Rudolph v. Hudson's Bay Co., No. 18-CV-8472 (PKC), 2019 WL 2023713, at *1 (S.D.N.Y. May 7, 2019) (direct purchase from defendants); In re Marriott, 440 F. Supp. 3d at 453-455 (patrons of

defendant); Castillo v. Seagate Tech., LLC, No. 16-CV-01958-RS, 2016 WL 9280242, at *1 (N.D. Cal. Sept. 14, 2016) (employees of defendant); In re Ambry Genetics Data Breach Litig., 567 F. Supp. 3d 1130, 1138 (C.D. Cal. 2021) (customers of defendants); Kirsten v. California Pizza Kitchen, Inc., No. 221CV09578DOCKES, 2022 WL 16894503, at *1 (C.D. Cal. July 29, 2022), reconsideration denied, No. 221CV09578DOCKES, 2022 WL 16894880 (C.D. Cal. Sept. 8, 2022) (employees of defendants).) There are no factual allegations about how Convergent got the PII at issue and it does not square with its role as a third-party debt collector with whom Plaintiffs have no consumer relationship. Plaintiffs cite no authority that would support their claim that if PII is provided to one entity with whom the plaintiff has a direct relationship, and that entity provides it to third party without any involvement of the plaintiff, the third party has a contractual relationship with the plaintiff. Without more information about the provision of the PII from the entity to the third party and the plaintiff's relationship with the third party, the Court cannot find a contractual relationship.

The Court GRANTS the Motion and DISMISSES this claim.

D. Breach of Duty of Confidence

Convergent seeks dismissal of Plaintiffs' breach of the duty of confidentiality claim. The Court agrees.

Plaintiffs are correct that Washington recognizes a common law duty of confidentiality. (See Resp. at 12 (citing Boeing Co. v. Sierracin Corp., 108 Wn.2d 38, 48 (1987); Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1205, 1212 (E.D. Wash. 2003); Modumetal, Inc. v. Xtalic Corp., 4 Wn. App. 2d 1029 (2018)).) But Plaintiffs fail to explain why these cases support their claim. Each of these cases generally identified a duty of confidentiality as a claim arising out of a contractual relationship. Plaintiffs have not explained how their claim fits this contractual framework or how they had an expectation that Convergent would keep the

1 information confidential. This is fatal to the claim. As one district court decision on which
 2 Plaintiffs rely noted, no Washington case has imposed a duty of confidentiality in the context of
 3 a data breach. See In re Capital One, 488 F. Supp. 3d at 409 n.21. Because Plaintiffs have failed
 4 to articulate how Convergent owed or breached this duty of confidentiality, the Court GRANTS
 5 the Motion and DISMISSES this claim.

6 **E. Invasion of Privacy**

7 Convergent argues that Plaintiffs' invasion of privacy claim must fail because Plaintiffs
 8 have failed to allege an intent to publish their PII or that the PII has reached a broad audience.
 9 Convergent is incorrect. Intentionality need not be alleged and the allegations as to the scope of
 10 the publication of Plaintiffs' PII is sufficiently broad to satisfy the elements of the claim.

11 Washington recognizes a common law right of privacy and individuals may bring a cause
 12 of action for invasion of that right. Reid v. Pierce Cnty., 136 Wn.2d 195, 206 (1998). The claim
 13 generally requires the plaintiff to prove that the defendant publicized a "matter concerning the
 14 private life of another" where the information publicized: "(a) would be highly offensive to a
 15 reasonable person, and (b) is not of legitimate concern to the public." Id. (citing Restatement
 16 (Second) of Torts § 652D (1977)). "[I]nvasion of privacy action is primarily concerned with
 17 compensating for injured feelings or mental suffering." Eastwood v. Cascade Broad. Co., 106
 18 Wn.2d 466, 471 (1986). Although there is no Washington State Supreme Court authority directly
 19 on point, the Washington State Court of Appeals has held that invasion of privacy is not an
 20 intentional tort and requires no proof of intentionality. Emeson v. Dep't of Corr., 194 Wn. App.
 21 617, 638 (Div. 3 2016) ("The tort invasion of privacy by publication does not include intent as an
 22 essential element."). And the Supreme Court has also found that an invasion of privacy claim can
 23 be brought even if the matter was not broadly publicized. See Reid, 136 Wn.2d at 212
 24

(approving an invasion of privacy claim premised on the Medical Examiner's Office employees' displaying of photographs of an autopsy at cocktail parties and in personal scrap books).

Plaintiffs have sufficiently alleged an invasion of privacy claim. They allege that Convergent disclosed Plaintiffs' PII by failing to secure it. (CAC ¶ 251.) While the publication allegations may be thin, there is enough here to suggest that Convergent at least unintentionally published the information. And Plaintiffs Guy and Tanner allege that their PII has already been accessed as a result of this breach. These allegations suffice given that intentionality is not requirement. And Plaintiffs also allege that the information is sensitive in nature and concerns their private lives, in large part because it includes social security numbers for which there is no general public interest, and its publication may be considered highly offensive. (CAC ¶ 53.) While a jury might disagree, the Court finds these allegations sufficient. And Convergent is incorrect that the publication must be to a large group. It is enough to know the information was accessed and is likely being disseminated. The Court DENIES the Motion as to this claim.

The Court also finds the damage allegations sufficiently detailed to confer Article III standing on Plaintiffs. They have alleged a concrete injury to their privacy that is fairly traceable to Convergent's failure to safeguard and allow the publication of their PII.

F. Unjust Enrichment

Convergent's attack to Plaintiffs' unjust enrichment claim falls short, and the claim is sufficiently pleaded.

"Unjust enrichment is the method of recovery for the value of the benefit retained absent any contractual relationship because notions of fairness and justice require it." Young, 164 Wn.2d at 484. A claim based on unjust enrichment requires proof of the following elements: "(1) the defendant receives a benefit, (2) the received benefit is at the plaintiff's expense, and (3) the

1 circumstances make it unjust for the defendant to retain the benefit without payment.” Id. at 484–
 2 85.

3 Plaintiffs have adequately alleged facts sufficient to satisfy all three elements of their
 4 unjust enrichment claim. First, Convergent is alleged to have obtained Plaintiffs’ PII in order to
 5 perform third-party debt collection services from which it derives financial gain. (CAC ¶ 258.)
 6 Although Convergent did not get the information directly from Plaintiffs, courts have held that
 7 benefits conferred through a third party may be sufficient. See Weinberg v. Advanced Data
 8 Processing, Inc., 147 F. Supp. 3d 1359, 1368 (S.D. Fla. 2015); In re Flonase Antitrust Litig., 692
 9 F. Supp. 2d 524, 544 (E.D. Pa. 2010). The same logic applies here, as the Court examines the
 10 benefit conferred, regardless of whether it was direct or indirect benefit. Second, Convergent is
 11 alleged to have obtained the PII at Plaintiffs’ expense at least insofar as it did not benefit
 12 Plaintiffs to have their PII lost to a third-party. Indeed, Plaintiffs allege that their PII has lost
 13 value as a result. Third, it is reasonable to allow a jury to determine whether the circumstances
 14 make it unjust for Convergent to retain the benefit without payment. See In re Capital One, 488
 15 F. Supp. 3d at 412 (noting that “courts have concluded that the failure to secure a party’s data
 16 can give rise to an unjust enrichment claim where a defendant accepts the benefits accompanying
 17 plaintiff’s data and does so at the plaintiff’s expense by not implementing adequate safeguards,
 18 thereby making it inequitable and unconscionable to permit defendant to retain the benefit of the
 19 data (and any benefits received therefrom), while leaving the plaintiff party to live with the
 20 consequences.” (citation and quotation omitted)).

21 Additionally, the Court finds the alleged injury sufficient to confer Article III standing.
 22 Plaintiffs allege that Convergent obtained their PII to their detriment because the PII lost value
 23
 24

on account of Convergent's misconduct. This is a sufficiently concrete injury traceable to Convergent's conduct that satisfies Article III standing.

The Court DENIES the Motion as to this claim.

G. Washington Consumer Protection Act

Plaintiffs have stated a claim under the Washington Consumer Protection Act (CPA) and the Court DENIES the Motion as to the claim.

Washington's CPA prohibits "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." RCW 19.86.020. "To prevail in a private CPA claim, the plaintiff must prove (1) an unfair or deceptive act or practice, (2) occurring in trade or commerce, (3) affecting the public interest, (4) injury to a person's business or property, and (5) causation." Panag v. Farmers Ins. Co. of Wash., 166 Wn.2d 27, 37 (2009). Failure to satisfy even one element is fatal to a CPA claim. Hangman Ridge Training Stables, Inc. v. Safeco Title Ins. Co., 105 Wn.2d 778, 784 (1986).

Citing the liberal construction of the CPA and the breadth of what constitutes an unfair act, the Court in Veridian concluded that the failure to take proper measures to secure PII can constitute an unfair act under the CPA. See Veridian, 295 F. Supp. 3d at 1161-62. Plaintiffs' allegations of Convergent's failure to secure their PII sufficiently identifies an unfair act that satisfies this element of the CPA.

Additionally, the Court finds that Plaintiffs have alleged a damage to their business or property sufficient to satisfy this element and Article III standing. Plaintiffs assert that the diminished value of their PII and the lost time spent remedying the PII disclosure are compensable. The allegations of the lost value of the PII are sufficient to show an injury, because "the injury requirement is met upon proof the plaintiff's property interest or money is diminished

1 because of the unlawful conduct even if the expenses caused by the statutory violation are
 2 minimal.” Panag, 166 Wn.2d at 57 (citation and quotation omitted). And even though the alleged
 3 lost time may not be evidence of an injury, it is evidence of damages. See id. (“‘Injury’ is distinct
 4 from ‘damages.’”) Plaintiffs have alleged an injury from the lost value of the PII and this
 5 satisfies both the CPA element and Article III standing, given that it is a concrete injury fairly
 6 traceable to Convergent’s alleged misconduct.

7 The Court DENIES the Motion as to this claim.

8 **H. Washington Data Breach Law**

9 Convergent seeks dismissal of Plaintiffs’ claims under Washington’s Data Breach Act,
 10 RCW 19.255. The Court agrees the claim is flawed and must be dismissed.

11 Plaintiffs invoke the Data Breach Act, RCW 19.255.010(2), which states:

12 Any person or business that maintains or possesses data that may include personal
 13 information that the person or business does not own or license shall notify the owner or
 14 licensee of the information of any breach of the security of the data immediately
 following discovery, if the personal information was, or is reasonably believed to have
 been, acquired by an unauthorized person.

15 RCW 19.255.010(5). The Act also provides that “[n]otification to affected consumers under this
 16 section must be made in the most expedient time possible, without unreasonable delay, and no
 17 more than thirty calendar days after the breach was discovered, unless the delay is at the request
 18 of law enforcement as provided in subsection (3) of this section, or the delay is due to any
 19 measures necessary to determine the scope of the breach and restore the reasonable integrity of
 20 the data system.” RCW 19.255.010(8). And the Act allows “[a]ny consumer injured by a
 21 violation of this chapter [to] institute a civil action to recover damages.” RCW 19.255.040(3)(a).

22 Convergent argues that Plaintiffs cannot pursue claims under RCW 19.255.010(2)
 23 because it only “pertains to owners or licensees of personal information.” (Mot. at 16.) This is
 24 correct. Plaintiffs have not alleged that Convergent maintains the PII without owning or licensing

1 it. The failure to include these allegations is fatal to the claim. Plaintiffs' claims under Section 2
2 are DISMISSED.

3 Plaintiffs argue that they may be able to satisfy RCW 19.255.010(1), which requires a
4 business to notify any resident of Washington of the breach. But no such claim has been asserted
5 and this cannot save the claim. Even if such a claim had been asserted, the Court would dismiss
6 it because none of named Plaintiffs is a resident of Washington—a requisite element.

7 The Court GRANTS the Motion and DISMISSES the claim.

8 **I. California Consumer Privacy Act**

9 Convergent seeks dismissal of Plaintiffs' California Consumer Privacy Act (CCPA) on
10 the theory that Plaintiffs failed to provide pre-suit notice. The Court agrees in part.

11 The CCPA provides a cause of action for those whose PII is subject to a theft,
12 unauthorized access, or exfiltration filtration. The CCPA states:

13 Any consumer whose nonencrypted and nonredacted personal information, as defined in
14 subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, or whose
15 email address in combination with a password or security question and answer that would
16 permit access to the account is subject to an unauthorized access and exfiltration, theft, or
disclosure as a result of the business's violation of the duty to implement and maintain
reasonable security procedures and practices appropriate to the nature of the information
to protect the personal information may institute a civil action for any of the following:

17 (A) To recover damages in an amount not less than one hundred dollars (\$100) and not
18 greater than seven hundred and fifty (\$750) per consumer per incident or actual damages,
whichever is greater.

19 (B) Injunctive or declaratory relief.

20 (C) Any other relief the court deems proper.

21 Cal. Civ. Code § 1798.150(a)(1) (West)

22 The CCPA includes a pre-suit notice provision, stating: "Actions pursuant to this section
23 may be brought by a consumer if, prior to initiating any action against a business for statutory
24 damages on an individual or class-wide basis, a consumer provides a business 30 days' written

1 notice identifying the specific provisions of this title the consumer alleges have been or are being
2 violated.” Cal. Civ. Code § 1798.150(b) (West). No notice is required if the consumer pursues
3 “an action solely for actual pecuniary damages suffered as a result of the alleged violations of
4 this title.” Id. At least one court considering the notice provision of the CCPA has concluded that
5 the notice is required as a condition precedent before filing suit so that the defendant can attempt
6 to cure the defect. Griffey v. Magellan Health Inc., No. CV-20-01282-PHX-MTL, 2022 WL
7 1811165, at *6 (D. Ariz. June 2, 2022). The court in Griffey dismissed the claim with prejudice,
8 but without any explanation. Id.

9 Plaintiffs correctly argue that the pre-suit notice is not applicable to this action because
10 they are only seeking “pecuniary damages”—i.e., non-statutory damages. Plaintiffs’ failure to
11 provide pre-suit notice for such a claim is not fatal to the claim. And the court DENIES the
12 Motion as to this aspect of the CCPA claim.

13 Plaintiffs also insist that they seek statutory damages under the CCPA. But Plaintiffs have
14 not provided pre-suit notice, and this bars the claim. Recognizing this impediment, Plaintiffs ask
15 the Court to dismiss this aspect of its CCPA without prejudice so they can attempt to cure the
16 defect. The Court agrees that dismissal should be without prejudice. This accords with the
17 remedial nature of the CCPA’s notice provision. Allowing a notice would give Convergent the
18 opportunity afforded to it under the CCPA to cure the injury. Other than Griffey, Convergent
19 provides no authority that would compel dismissal with prejudice. And the Court declines to
20 follow the outcome in Griffey because the court there provided no explanation as to why it
21 dismissed the claim with prejudice or why doing so would align with the purpose of the CCPA.
22 The Court declines to follow the Griffey decision, and DISMISSES Plaintiffs’ CCPA claim for
23 statutory damages without prejudice.
24

1 Convergent also argues that Plaintiffs have not identified actionable damages. The Court
2 disagrees. Plaintiffs have alleged a diminution of the value of their PII. These allegations are
3 sufficient to show damages which are fairly traceable to Convergent's violation of the CCPA.
4 This satisfies the damages requirement and Article III standing.

5 In sum, the Court GRANTS in part and DENIES in part the Motion. The CCPA claim for
6 pecuniary damages may proceed, but the claim for statutory damages is dismissed without
7 prejudice for lack of pre-suit notice.

8 **J. California Unfair Competition Law**

9 Convergent seeks dismissal of Plaintiffs' California Unfair Competition Law (UCL)
10 claims on the theory that Plaintiffs have not alleged an adequate personal injury and they have
11 not alleged a statutory violation. The Court disagrees.

12 "The UCL prohibits, and provides civil remedies for, unfair competition, which it defines
13 as "any unlawful, unfair or fraudulent business act or practice." Kwikset Corp. v. Superior Ct.,
14 51 Cal. 4th 310, 323, 246 P.3d 877 (2011) (quoting Cal. Bus. & Prof. Code § 17200). "[A]
15 person who has suffered injury in fact and has lost money or property as a result of the unfair
16 competition" may file suit. Cal. Bus & Prof. Code § 17204. The UCL requires "that a plaintiff
17 have 'lost money or property' to have standing to sue." Kwikset, 51 Cal. 4th at 323. "There are
18 innumerable ways in which economic injury from unfair competition may be shown." Id. "A
19 plaintiff may (1) surrender in a transaction more, or acquire in a transaction less, than he or she
20 otherwise would have; (2) have a present or future property interest diminished; (3) be deprived
21 of money or property to which he or she has a cognizable claim; or (4) be required to enter into a
22 transaction, costing money or property, that would otherwise have been unnecessary." Id. The
23 injury need not be significant to satisfy the requirement. Id. at 324.

1 The Court agrees with Plaintiffs that this claim is adequately pleaded. First, the Court
 2 finds that Plaintiffs have alleged a sufficient injury to pursue the claims. Plaintiffs have pointed
 3 out that their PII has lost value by virtue of the breach. This is an economic injury sufficient
 4 under the UCL. Second, just as the Court finds Plaintiffs alleged an actionable unfair business
 5 practice under the Washington CPA, the Court finds Plaintiffs have adequately alleged that
 6 Convergent's failure to protect their PII is an unfair business practice under the UCL. The Court
 7 DENIES the Motion as to this claim.

8 **K. California Invasion of Privacy**

9 Convergent correctly seeks dismissal of Plaintiffs' California Invasion of Privacy claim.

10 The California Constitution provides that "[a]ll people are by nature free and independent
 11 and have inalienable rights," including "pursuing and obtaining safety, happiness, and privacy."
 12 CAL. CONST. art. I, § 1. To establish a claim for violation of the right to privacy under article I,
 13 § 1, a plaintiff must establish "(1) a legally protected privacy interest; (2) a reasonable
 14 expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious
 15 invasion of privacy." Hill v. Nat'l Collegiate Athletic Assn., 7 Cal.4th 1, 39–40, 26 Cal.Rptr.2d
 16 834, 865 P.2d 633 (1994). "To be 'serious,' the invasion must constitute an 'egregious breach of
 17 the social norms underlying the privacy right.'" Doe v. Beard, 63 F. Supp. 3d 1159, 1169 (C.D.
 18 Cal. 2014) (quoting Hill, 7 Cal.4th at 37). "Plaintiffs must show more than an intrusion upon
 19 reasonable privacy expectations." Id. "Actionable invasions of privacy also must be 'highly
 20 offensive' to a reasonable person. . . ." Hernandez v. Hillsides, Inc., 47 Cal.4th 272, 295, 97
 21 Cal.Rptr.3d 274, 211 P.3d 1063 (2009).

22 Although an intentional disclosure is usually required, a negligent disclosure of highly
 23 sensitive information, especially where a statute may criminalize the disclosure of such
 24

1 information, may sustain a claim. See Doe, 63 F. Supp. 3d at 1170 (finding that negligent
2 disclosure of HIV-positive status was sufficient to satisfy the final element, particularly given the
3 criminalization of such a disclosure); Stasi v. Inmediata Health Grp. Corp., 501 F. Supp. 3d 898,
4 926 (S.D. Cal. 2020) (finding allegations that defendant posted plaintiffs’ medical information
5 online sufficiently stated a claim); In re Ambry, 567 F. Supp. 3d at 1143 (finding allegations of a
6 failure to protect medical information from third-party exfiltration stated a California
7 constitutional invasion of privacy claim).

8 Plaintiffs’ California constitutional claim fails because they have not alleged a “highly
9 offensive” disclosure of their PII. While intentionality may not be required, courts have only
10 permitted negligent invasion of privacy claims when the nature of the information was highly
11 sensitive and could cause great humiliation. See Doe, 63 F. Supp. 2d at 1169. While the PII
12 contains sensitive information including financial information and Social Security numbers, it
13 does not include medical information or any particularly sensitive information whose revelation
14 could cause serious harm or outrage. See id. Plaintiffs point to no court that has sustained this
15 kind of claim as to PII, and they instead rely on cases involving disclosure of personal medical
16 information, not financial information or Social Security information. As one court considering
17 similar claims, “[e]ven negligent conduct that leads to theft of highly personal information,
18 including social security numbers, does not approach the standard of actionable conduct under
19 the California Constitution. . . .” In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1063
20 (N.D. Cal. 2012). The Court follows this same reasoning and GRANTS the Motion and
21 DISMISSES this claim.

22
23
24

1 **L. Declaratory Relief**

2 Convergent asks the Court to dismiss the declaratory relief Plaintiffs request for lack of
3 any viable claims. But given the Court's conclusions above, this argument lacks merit. Plaintiffs
4 may seek declaratory relief and DENIES the Motion as to this requested relief.

5 **CONCLUSION**

6 The Court GRANTS in part and DENIES in part Convergent's Motion to Dismiss. The
7 Court GRANTS the Motion in part and DISMISSES Plaintiffs' negligence, breach of implied
8 contract, breach of the duty of confidence, Washington Data Breach Law, CCPA (in part) and
9 California constitutional privacy claims. The Court DENIES the Motion as to Plaintiffs' invasion
10 of privacy, unjust enrichment, Washington CPA, CCPA (in part), UCL, and declaratory relief
11 claims. The Court DISMISSES all but the CCPA claim with prejudice. If Plaintiffs wish to file
12 an amended complaint, they must do so within 45 days of this Order. The Court will separately
13 issue an order requiring a joint status report in the interim.

14 The clerk is ordered to provide copies of this order to all counsel.

15 Dated July 20, 2023.

16 

17 Marsha J. Pechman
18 United States Senior District Judge
19
20
21
22
23
24